

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(43) 国际公布日:
2001年3月1日(01.03.2001)

PCT

(10) 国际公布号:
WO 01/15024 A1

(51) 国际分类号: G06F 17/60, G07F 7/08, G07G 1/12

(21) 国际申请号: PCT/CN99/00124

(22) 国际申请日: 1999年8月23日(23.08.1999)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71)(72) 发明人/申请人: 李东声(LI, Dongsheng) [CN/CN];
中国北京市上地信息产业基地创业中路四街26号4层,
Beijing 100085 (CN).

(74) 代理人: 北京三友专利代理有限公司(BEIJING
SANYOU PATENT AGENCY CO., LTD.); 中国北京
市北三环中路40号, Beijing 100088 (CN).

(81) 指定国(国家): AE, AL, AM, AT, AU, AZ, BA, BB, BG,
BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI,

GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP,
KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV,
MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO,
RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA,
UG, US, UZ, VN, YU, ZA, ZW

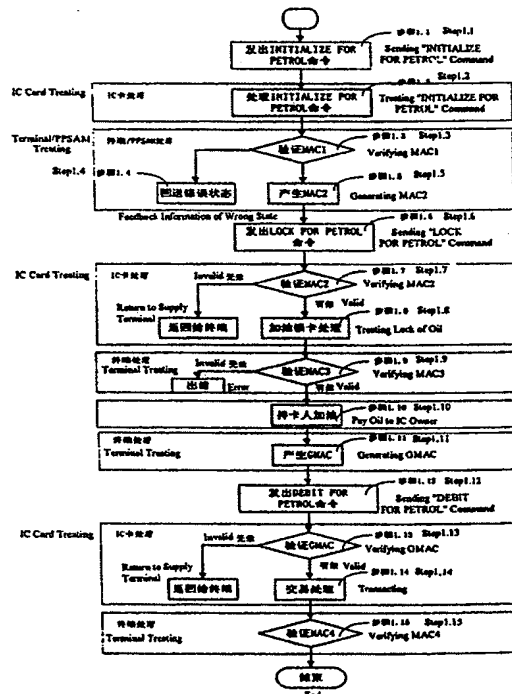
(84) 指定国(地区): ARIPO专利(GH, GM, KE, LS, MW,
SD, SZ, UG, ZW), 欧亚专利(AM, AZ, BY, KG, KZ,
MD, RU, TJ, TM), 欧洲专利(AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT,
SE), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN,
GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号, 请参考刊登在每期
PCT公报期刊起始的“代码及缩写符号简要说明”。

(54) Title: A METHOD FOR THE ACCOMPLISHMENT SECURE TRANSACTION FOR
ELECTRONICBANKBOOK (PURSE)

(54) 发明名称: 一种实现电子存折(钱包)安全交易的方法



(57) Abstract: The present invention related to a method for accomplishment secure transaction for electronic bankbook (purse), characterized by that a grey lock mark is incorporated into the electronic bankbook (purse) as one of its properties. While the grey lock mark is set in an IC card, the source of locking IC card is written in the IC card. During the operation to deduct the paid money from a sum of money, the step to confirm the source of the IC card is executed, and the operation to deduct the paid money from a sum of money and the operation to unlock IC card from the greylock are combined into one operation of IC card, namely, after the paid money is successfully deducted, the grey lock mark is automatically removed. The problem that the grey lock is illicitly removed is effectively solved, as a result, a consumption transaction process of the electronic bankbook (purse) is safer and easier.

[见续页]



WO 01/15024 A1



(57) 摘要

本发明系关于一种实现电子存折（钱包）安全交易的方法，其特征在于：将灰锁标记并入该电子存折（钱包），成为该电子存折（钱包）的属性参数之一；在灰锁 IC 卡即置灰锁标记的同时，将锁卡的来源记入 IC 卡；当扣款操作时执行对该锁卡来源的判断，并将扣款操作和解灰操作合并为 IC 卡上的一步操作，即扣款成功后自动解灰。从而彻底有效地解决非法解锁的问题，使电子存折（钱包）的消费交易过程更加安全顺畅。

一种实现电子存折（钱包）安全交易的方法

技术领域

本发明涉及 IC 卡应用领域，特别是作为金融 IC 卡应用的电子存折或电子钱包的应用领域中，一种售前交易的电子存折（钱包）的安全认证实现方法。

5 发明背景

目前，IC 卡的应用越来越普及，范围也越来越广泛，由于其使用方便、便于携带、运行快捷、安全可靠等特点而越来越受到更多使用者的欢迎，特别是在自助的环境下。

但是，现有的采用 IC 卡的支付系统针对的主要是售后交易，即支付方在支付
10 后获得服务，如商场购物。而对售前交易，即支付方先获得服务后支付，如 IC 卡加油，则在安全保证上存在有漏洞，尤其是自助环境下的售前服务。现以 IC 卡加油为例作进一步说明：

依照现有的一般 IC 卡支付系统，在用 IC 卡加油时，其流程为：用户插卡、IC 卡与终端的双向认证、用户加油、加油结束、终端从 IC 卡扣款。从上面的流程中可
15 以看出，在从用户开始加油到终端从 IC 卡扣款成功这一段较长的时间内，如果出现 IC 卡被从读卡器中拔出、中途断电或终端意外故障等情况，引起终端对 IC 卡扣款操作无法进行下去（这种情形统称逃卡）时，会引起一系列的问题。而加油环境下受其行业的防爆规范限制，采用全吞式读卡器，成本很高，难以推广。

为解决这一问题，现有的 IC 卡加油支付系统均引入了灰锁的概念。灰锁是指
20 在 IC 卡上作一个特定的标记，以标识 IC 卡在上次使用时的使用情况。若 IC 卡上的灰锁标记（简称灰标记）被清除，说明这张 IC 卡在上次交易中正常结束操作，可以继续使用；若 IC 卡上存在灰锁标记，则说明在上次使用时，交易并没有正常结束，这张 IC 卡（称为灰卡）若要继续使用，必须先将该灰锁标记清除（解灰锁，简称解灰），如果上次没有从这张卡上扣除所需的金额，则还需先补扣上次交易金额来平
25 帐。

因此，上述的 IC 卡加油交易流程就变为：用户插卡、IC 卡与终端的双向认证、

判断是否灰卡、若不是灰卡则灰锁 IC 卡、用户加油、加油结束、终端从 IC 卡扣款、终端对 IC 卡解灰锁。同时增加了解灰交易，其流程为：若 IC 卡是灰卡，查找相应的灰记录，判断灰记录与 IC 卡的匹配，若存在与 IC 卡相匹配的灰记录，则补扣灰记录中的交易额（如果需要），解灰锁。在上述交易流程中，由于扣款和解灰是分开操作的，因此仍存在有安全隐患：若能够仅仅操作灰标记而不进行扣款的话，对持卡人而言就能获利，而对发卡方而言就会蒙受损失。在此，引入“交易的获益方”这一概念加以深入说明。

根据对 IC 卡随意操作时的收益方，将交易（或对 IC 卡的操作）分为正方交易和负方交易。正方交易（或对 IC 卡的操作）是指那些如果可以随意操作的话，会对持卡人有利或对发卡人不利的交易（或对 IC 卡的操作），如圈存、更改透支限额、个人密码（PIN）解锁、更改 IC 卡上受保护的文件等；负方交易（或对 IC 卡的操作）是指那些如果可以随意操作的话，会对持卡人不利或对发卡人有利的交易（或对 IC 卡的操作），如消费等。一般而言，正方交易的保护密钥存放在发卡方主机上，而负方交易的保护密钥可以存放在终端内，现有的常用方式是存放在终端的 PSAM 卡上。

根据正方交易和负方交易的定义，可以看出扣款操作是负方操作，密钥是可以存放在 PSAM 卡上的，而解灰操作是正方操作，密钥应保存在发卡方主机上。但是在正常的交易流程中又必须有解灰操作，且不可能联机进行，所以就出现了矛盾。解灰操作的密钥如果存放在 PSAM 卡上的话，由于 PASM 卡是一张 IC 卡，它只能用密钥被动的计算和认证，对解灰操作而言并不存在约束，这样就有 PSAM 被使用于非法解锁灰卡的可能。

现有技术的应用中，是将解灰密钥存放在终端的加密模组中，或将解灰密钥一部分存放在终端的加密模组中，一部分存放在终端的 PSAM 卡上。由于加密模组内部可以存放程序，具有一定的自主性，所以将解灰的操作内建在加密模组中，由它来实现对解灰的安全控制。为了实现加密模组对解灰的安全控制，就必须在服务前锁卡，即建立 IC 卡的灰锁标记。如果在中途发生逃卡，由终端通过网络将逃卡金额及当前余额上报，在解灰时就需要根据灰锁的标记及通过网络下发的脱逃金额及余额来判断补扣的金额，并在补扣后将 IC 卡解灰。这时又存在了新的问题：（1）IC 卡无法判断补扣金额的合法性，补扣金额的安全保障以只能由网络 and 终端来提供，所以存在较薄弱的安全环节；（2）如前所述，解锁操作是正方交易，而正方保护密钥

不得不存放在不受发卡方控制的应用环境下，对这部分密钥的安全管理对发卡方而言也是一个问题。

到目前为止，还没有一个彻底的解决方法来处理这种较为特殊的情况下的 IC 卡售前交易。

5 发明内容

从上面的分析可以看出：这个问题的核心是，IC 卡的扣款操作和灰锁操作两者是相对独立的。通常的解决方案是试图在两者间建立某种关联来把他们联系起来，而本发明的主要目的则在于从核心入手，将扣款操作和灰锁操作结合起来，使两者统一，从而提出一种新的实现售前交易的电子存折（钱包）安全交易的方法，彻底有效地解决上述问题。

本发明一种实现电子存折（钱包）安全交易的方法，是将灰锁标记并入该电子存折（钱包），成为该电子存折（钱包）的属性参数之一，当灰锁时，使除与解灰相关的操作以外，其它对该电子存折（钱包）的任何操作均无效。

本发明一种实现电子存折（钱包）安全交易的方法，在灰锁 IC 卡即置灰锁标记的同时，将锁卡的来源记入 IC 卡；当扣款操作时执行对该锁卡来源的判断，并将扣款操作和解灰操作合并为 IC 卡上的一步操作，即扣款成功后自动解灰。该锁卡来源贯穿整个交易流程。

根据本发明技术方案，更进一步的可在主机上保存有一条可以实现扣款操作和强制解灰操作的密钥，使灰锁后的 IC 卡可在联机的终端上通过联机方式实现补扣款和强制解灰操作。例如，如果终端出现故障而引起无法扣款或数据不能上传或这次记录丢失，该卡可以在联机的终端上通过联机方式将灰标记清除。

根据本发明方法建立的 IC 卡消费交易流程就变为：用户插卡、终端和 IC 卡双向认证、终端灰锁 IC 卡、消费交易、消费交易实现后终端从 IC 卡的电子存折（钱包）扣款并解灰锁。

上述灰锁 IC 卡是指：IC 卡根据其锁卡的来源生成一认证码，同时将产生该锁卡来源的所需参数传递给终端，由终端采用与 IC 卡相同的机制产生另一锁卡来源，并使用该锁卡来源生成另一认证码，将该认证码送入 IC 卡，IC 卡判断与上述 IC 卡自身生成的认证码是否相同，若相同时执行灰锁操作并将这次灰锁的特征码返回给

终端。该灰锁特征码为根据锁卡来源及包括终端描述信息在内的相应数据生成。

上述终端从 IC 卡的电子存折（钱包）扣款并解灰锁是指：终端根据其锁卡来源和扣款所需的参数生成一认证码，将该认证码与相应参数一并送入 IC 卡，IC 卡内部采用其自身的锁卡来源和相同的参数通过相同的机制产生另一认证码，判断该
5 认证码与终端产生的认证码一致就从 IC 卡的电子存折（钱包）上实现扣款，扣款成功的同时将灰标记清除。

终端更进一步可将扣款时所需的认证码和这次的逃卡金额及灰锁特征码共同作为这次灰记录的部分信息保存起来，并上传给中心机；如果某次交易过程未完整结束的未被扣款解灰的 IC 卡，下一次在任何一个保存有该灰记录的终端上使用时，
10 终端可先验证该灰锁特征码以确定 IC 卡上的锁卡来源与计算该条灰记录中的扣款认证码的锁卡来源相同，通过后执行补扣款解灰操作。

根据本发明技术方案，所述的锁卡来源为在 IC 卡上建立的一条过程密钥 SESPk，该过程密钥至少与一 IC 卡临时生成的伪随机数 ICC 相关。

上述的过程密钥 $SESPk = 3DES(DPK, DATA)$ ，其中 DPK 是电子存折（钱包）的
15 消费密钥，是由电子存折（钱包）消费主密钥 MPK 根据该 IC 卡的应用序号分散得到，每张 IC 卡由于其应用序号（卡号）不同而它们的 DPK 也各不相同。DATA 是特定的参数，包括有所述的 IC 卡临时生成的伪随机数 ICC、电子存折（钱包）的交易序号 CTC、终端交易序号 TTC 的最后两个字节。可见每次交易的 SESPk 由于 IC 卡的应用序号及 DATA 不同而各不相同，所以可以用 SESPk 得到可靠的灰锁来源。

当灰锁电子存折（钱包）时，终端将终端交易序号 TTC 送入 IC 卡，IC 卡获得自己的伪随机数 ICC 和电子存折（钱包）交易序号 CTC，内部建立过程密钥 SESPk，且将产生过程密钥 SESPk 的相应参数记录下来，产生这次灰锁特征码同时亦记录下来，将伪随机数 ICC、电子存折（钱包）交易序号 CTC 发给终端，终端的安全认证
20 模组或 PSAM 卡中存放有电子存折（钱包）消费主密钥 MPK，安全认证模组或 PSAM 卡根据 IC 卡应用序号推导出 IC 卡上该电子存折（钱包）的 DPK，再根据伪随机数 ICC、电子存折（钱包）交易序号 CTC、终端交易序号 TTC，采用与 IC 卡相同的机制建立起相同的过程密钥 SESPk；
25

扣款操作时终端使用该过程密钥 SESPk 根据扣款的金额、操作的日期时间等计算出认证码，一并送入 IC 卡，IC 卡内部采用相同的数据和算法使用过程密钥 SESPk

同样计算出认证码，与终端计算的结果相比较，相同则内部实现扣款和解灰；若认证码与终端计算的不同，内部不作操作，将内部出错计数器增加，返回出错代码，如果内部出错计数器到达一定的次数，将 IC 卡的应用内部锁定以防止恶意的试探。

根据本发明技术方案构思，将灰锁标记并入电子存折（钱包）成为一特殊的加油电子存折（钱包）时，除具备通常的读余额、圈存、圈提、消费/取现、改透支限
5 额等功能外，同时增加了加油消费、本地解灰锁和联机解灰锁功能。

描述该加油电子存折（钱包）的状态除通常的空闲状态、圈存状态、消费/取现状态、圈提状态、修改状态外，还存在预加油状态、灰锁状态、和解灰锁状态，并在电子存折（钱包）通常的命令集中增加了加油初始化、加油锁卡、加油消费、
10 解锁初始化、解锁、读取状态命令，其中，加油初始化命令用于初始化加油消费交易，加油锁卡命令用于灰锁加油消费电子存折（钱包），加油消费命令用于本地加油消费交易同时解灰锁，解锁初始化命令用于初始化联机解灰锁消费交易，解锁命令用于联机解灰锁交易同时补扣加油消费，读取状态命令用于读取灰锁状态并启动本地解灰锁交易。

15 采用本发明技术方案彻底解决了以往的问题：

由于解灰和扣款操作合二为一，正常操作的解灰密钥的管理隐患不再存在，可以本着负方交易的原则而存放在 PSAM 上。而在联机解灰时其操作的密钥本着正方交易的原则存放在主机上，它的管理隐患也不复存在。

由于解灰和扣款操作合二为一，非法解灰的问题一方面转变成了终端扣款准确性的问题，即只要认可终端执行扣款的金额是合法的，解灰就是合法的。在另一方面，当出现逃卡后补扣时，由于只有 IC 卡和出现逃卡的终端的 PSAM 才知道可以执行这次补扣的过程密钥 SESPk，而且终端的 PSAM 在交易结束后将不再保留 SESPk，所以在补扣时只有 IC 卡才可获知（内部恢复）这条密钥，扣款操作时的扣款认证码是产生逃卡的终端的 PSAM 在 SESPk 被清除之前计算好保存下来的，任何篡改这个认
20 证码或用以计算这个认证码的参数（如逃卡金额等）的举动都会造成补扣失败，而且 IC 卡的内部应用锁定机制又能防止外界的恶意试探，所以这转变成了 IC 卡的安全机制的问题，与应用彻底无关。

综上所述，整个解灰的问题转变成了终端和 IC 卡的可靠性的问题，而这两点都是能有效管理的，并且与现有的终端和 IC 卡的安全机制不存在冲突。

附图简要说明

图 1 为本发明实施例加油电子存折加油交易流程示意图。

图 2 为本发明实施例加油电子存折联机解灰锁交易流程示意图。

图 3 为本发明实施例加油电子存折本地解灰锁交易流程示意图。

5 实施本发明的方式

下面通过实施例及附图对再本发明进行详细阐述。

以 IC 卡加油支付系统为例。将在 IC 卡上需要与灰锁关联的电子存折与灰锁合并成为一个特殊的电子存折——加油电子存折，这个电子存折除具备一般电子存折的一切功能——读余额、圈存、圈提、消费/取现、改透支限额等，同时针对使用
10 IC 卡进行脱机加油消费存在灰锁的情形增加了加油消费、本地解灰锁和联机解灰锁的功能，解决了非法解锁包括直接去锁和篡改逃卡金额的问题，从而保证加油消费这种售前交易的顺畅安全进行。

加油电子存折的基本应用与一般电子存折的应用完全相同，在此请恕不予赘述。而加油消费、本地解灰锁和联机解灰锁作为基本应用的外延，使加油电子存折
15 应用增加了新的范畴，下面通过对其命令和交易流程的分别描述加以详细的说明。

在应用执行过程中，卡片总是处于某种状态之一，在一种状态下，只有某些命令能执行。卡片具有的状态有：空闲状态、圈存状态、消费/取现状态、圈提状态、修改状态、预加油状态、灰锁状态、解灰锁状态，其中的预加油状态、灰锁状态和解灰锁状态是加油电子存折特有的状态。

20 当应用选择完成后，应用首先进入空闲状态。当卡片从终端收到一条命令后，它必须检查当前状态是否允许。命令成功完成以后，卡片根据表 1 所示进入另一个状态（或同一个）。如果命令没有成功执行，卡片进入空闲状态。

表 1 说明了命令成功执行后的状态变化。第一行描述了命令发出时卡片的当前状态，第一列描述了发出的命令，而整张表给出了命令执行成功后的状态。

25 阴影部分指出命令在卡片处于相应状态时是无效的，在这种情况下，卡片不执行命令，并回应终端‘6901’状态——命令不接受（无效）状态。由于命令不能成功执行，所以若卡片原来处于灰锁，结果状态仍是灰锁，若卡片原来处于其他状态，

结果状态是空闲。

表1 命令执行成功后的状态变化

命令 \ 状态	空闲	圈存	消费/取现	圈提	修改	预加油	灰锁	解灰锁
圈存	N/A	空闲	N/A	N/A	N/A	N/A	N/A	N/A
消费/取现	N/A	N/A	空闲	N/A	N/A	N/A	N/A	N/A
圈提	N/A	N/A	N/A	空闲	N/A	N/A	N/A	N/A
读余额	空闲	圈存	消费/取现	圈提	修改	加油消费	灰锁	解灰锁
取交易认证	空闲	圈存	消费/取现	圈提	修改	加油消费	灰锁	解灰锁
圈存初始化	圈存	圈存	圈存	圈存	圈存	圈存	N/A	N/A
消费初始化	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现	N/A	N/A
取现初始化	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现	N/A	N/A
圈提初始化	圈提	圈提	圈提	圈提	圈提	圈提	N/A	N/A
修改初始化	修改	修改	修改	修改	修改	修改	N/A	N/A
修改透支限额	N/A	N/A	N/A	N/A	空闲	N/A	N/A	N/A
加油初始化	预加油	预加油	预加油	预加油	预加油	预加油	N/A	N/A
加油锁卡	N/A	N/A	N/A	N/A	N/A	灰锁	N/A	N/A
加油消费	N/A	N/A	N/A	N/A	N/A	N/A	空闲	N/A
解锁初始化	N/A	N/A	N/A	N/A	N/A	N/A	解灰锁	解灰锁
解锁	N/A	N/A	N/A	N/A	N/A	N/A	N/A	空闲
读取状态	N/A	N/A	N/A	N/A	N/A	N/A	灰锁	N/A

表 2 定义了命令类别和命令字节的编码, 以及加油电子存折应用使用的参数

- 5 P1 和 P2。在该命令集中, 除通常电子存折所具有的命令外, 新增加了加油初始化、加油锁卡、加油消费、解锁初始化、解锁、读取状态命令, 其中, 加油初始化命令用于初始化加油消费交易, 加油锁卡命令用于灰锁加油消费电子存折, 加油消费命令用于本地加油消费交易同时解灰锁, 解锁初始化命令用于初始化联机解灰锁消费交易, 解锁命令用于联机解灰锁交易同时补扣加油消费, 读取状态命令用于读取灰锁状态。
- 10 下面分别对该等新增加的命令以及响应作出详细描述。而其它常规的命令与现有技术应用相同, 请恕不再赘述。

表2 命令的类别字节和指令字节

命令	CLA	INS	P1	P2
修改个人密码	'80'	'5E'	'01'	'00'
圈存	'80'	'52'	'00'	'00'
消费/取现	'80'	'54'	'01'	'00'
圈提	'80'	'54'	'03'	'00'
读余额	'80'	'5C'	'00'	'0X'
取交易认证	'80'	'5A'	'00'	'XX'
取现初始化	'80'	'50'	'02'	'01'
圈存初始化	'80'	'50'	'00'	'0X'
消费初始化	'80'	'50'	'01'	'0X'
圈提初始化	'80'	'50'	'05'	'01'
修改透支限额初始化	'80'	'50'	'04'	'01'
重装个人密码	'80'	'5E'	'00'	'00'
修改透支限额	'80'	'58'	'00'	'00'
*加油初始化	'E0'	'50'	'01'	'01'
*加油锁卡	'E0'	'50'	'02'	'01'
*加油消费	'E0'	'54'	'01'	'00'
*解锁初始化	'E0'	'50'	'03'	'01'
*解锁	'E0'	'54'	'01'	'01'
*读取状态	'E0'	'50'	'04'	'01'

1、加油初始化（INITIALIZE FOR PETROL）命令：INITIALIZE FOR PETROL 命令用于初始化加油消费交易，其命令报文见表 3，命令报文的数据域见表 4。此命令执行成功的响应报文数据域见表 5。如果命令执行不成功，则只在响应报文中回送 SW1 和 SW2。此命令执行成功的响应报文的状态码是 '9000'。表 6 描述了 IC 卡可能回送的错误状态。其中 ED 为电子存折。

表 3 INITIALIZE FOR PETROL 命令报文

代码	值
CLA	'E0'
INS	'50'
P1	'01'
P2	'01' 用于加油交易；其他值保留
L _r	'0B'
Data	见表 4
L _c	'10'

表 4 INITIALIZE FOR PETROL 命令报文数据域

说明	长度 (字节)
密钥索引	1
终端机编号	6
终端交易序号	4

表 5 INITIALIZE FOR PETROL 响应报文数据域

说明	长度 (字节)
ED 余额	4
ED 脱机交易序号	2
密钥版本	1
算法标识	1
伪随机数 (ICC)	1
MAC1	4

表 6 INITIALIZE FOR PETROL 错误状态

SW1	SW2	说明
'69'	'01'	命令不接受 (无效状态, 即灰锁原已建立)
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'94'	'03'	密钥索引不支持
'94'	'02'	交易计数器到达最大值

2、加油锁卡 (LOCK FOR PETROL) 命令: LOCK FOR PETROL 命令用于灰锁加油消费电子存折。其命令报文见表 7。命令报文的数据域见表 8。此命令执行成功的响应报文数据域见表 9。如果命令执行不成功, 则只在响应报文中回送 SW1 和 SW2。此命令执行成功的状态码是 '9000'。表 10 描述了 IC 卡可能回送的错误状态。

表 7 LOCK FOR PETROL 命令报文

代码	值
CLA	'E0'
INS	'50'
P1	'02'
P2	'01'
L _c	'0B'
Data	见表 8
L _c	'08'

表 8 LOCK FOR PETROL 命令报文数据域

说明	长度 (字节)
交易日期 (终端)	4
交易时间 (终端)	3
MAC2	4

表 9 LOCK FOR PETROL 响应报文数据域

说明	长度 (字节)
TAC	4
MAC3	4

表 10 LOCK FOR PETROL 错误状态

SW1	SW2	说明
'69'	'01'	命令不接受 (无效状态)
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'93'	'02'	MAC 无效

3、加油消费 (DEBIT FOR PETROL) 命令: DEBIT FOR PETROL 命令用于本地加油消费交易, 同时解灰锁。其命令报文见表 11。命令报文的数据域见表 12。此命令执行成功的响应报文数据域见表 13。如果命令执行不成功, 则只在响应报文中回送 SW1 和 SW2。此命令执行成功的状态码是 '9000'。表 14 描述了 IC 卡可能回送的错误状态。

表 11 DEBIT FOR PETROL 命令报文

代码	值
CLA	'E0'
INS	'54'
P1	'01'
P2	'00'
Lc	'19'
Data	见表 12
Lc	'08'

表 12 DEBIT FOR PETROL 命令报文数据域

说明	长度 (字节)
交易金额	4
ED 脱机交易序号	2
终端机编号	6
终端交易序号	4
交易日期 (终端)	4
交易时间 (终端)	3
GMAC	4

表 13 DEBIT FOR PETROL 响应报文数据域

说明	长度 (字节)
TAC	4
MAC4	4

表 14 DEBIT FOR PETROL 错误状态

SW1	SW2	说明
'69'	'01'	命令不接受 (无效状态)
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'67'	'00'	长度错误
'93'	'02'	MAC 无效

4、解锁初始化 (INITIALIZE FOR UNLOCK) 命令: INITIALIZE FOR UNLOCK 命令用于初始化联机解灰锁消费交易。其命令报文见表 15。命令报文的数据域见表 16。此命令执行成功的响应报文数据域见表 17。如果命令执行不成功, 则只在响应报文中回送 SW1 和 SW2。此命令执行成功的状态码是 '9000'。表 18 描述了 IC 卡可能回送的错误状态。

表 15 INITIALIZE FOR UNLOCK 命令报文

代码	值
CLA	'E0'
INS	'50'
P1	'03'
P2	'01' 用于加油交易; 其他值保留
L _r	'07'
Data	见表 16
L _c	'10'

表 16 INITIALIZE FOR UNLOCK 命令报文数据域

说明	长度 (字节)
密钥索引	1
终端机编号	6

表 17 INITIALIZE FOR UNLOCK 响应报文数据域

说明	长度 (字节)
ED 余额	4
ED 脱机交易序号	2
密钥版本	1
算法标识	1
伪随机数 (ICC)	4
MAC1	4

表 18 INITIALIZE FOR UNLOCK 错误状态

SW1	SW2	说明
'69'	'01'	命令不接受 (无效状态, 即灰锁未建立)
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'94'	'03'	密钥索引不支持
'94'	'02'	交易计数器到达最大值

5、解锁 (DEBIT FOR UNLOCK) 命令: DEBIT FOR UNLOCK 命令用于联机解灰锁交易, 同时补扣加油消费。其命令报文见表 19。命令报文的数据域见表 20。此命令执行成功的响应报文数据域见表 21。如果命令执行不成功, 则只在响应报文中回送 SW1 和 SW2。此命令执行成功的状态码是 '9000'。表 22 描述了 IC 卡可能回送的错误状态。

表 19 DEBIT FOR UNLOCK 命令报文

代码	值
CLA	'E0'
INS	'54'
P1	'01'
P2	'01'
Lc	'0F'
Data	见表 20
Lr	'04'

表 20 DEBIT FOR UNLOCK 命令报文数据域

说明	长度 (字节)
交易金额	4
交易日期 (主机)	4
交易时间 (主机)	3
MAC2	4

表 21 DEBIT FOR UNLOCK 响应报文数据域

说明	长度 (字节)
MAC3	4

表 22 DEBIT FOR UNLOCK 错误状态

SW1	SW2	说明
'69'	'01'	命令不接受 (无效状态)
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'67'	'00'	长度错误
'93'	'02'	MAC 无效

6、读取状态 (GET GREY STATUS) 命令: GET GREY STATUS 命令用于获得存折
5 的灰状态。其命令报文见表 23。命令报文的数据域不存在。此命令执行成功的响应
报文数据域见表 24。如果命令执行不成功, 则只在响应报文中回送 SW1 和 SW2。此
命令执行成功的状态码是 '9000'。 表 25 描述了 IC 卡可能回送的错误状态。

表 23 GET GREY STATUS 命令报文

代码	值
CLA	'E0'
INS	'50'
P1	'04'
P2	'01'
Lc	不存在
Data	不存在
Lr	'11'

表 24 GET GREY STATUS 响应报文数据域

说明	长度 (字节)
Grey Flag	1
ED 余额	4
ED 脱机交易序号	2
ED 联机交易序号	2
MAC3	4
TAC	4

MAC3 和 TAC 是 GREY LOCK 时 IC 卡返回的值。

表 25 GET GREY STATUS 错误状态

SW1	SW2	说明
'69'	'01'	命令不接受 (无效状态)
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'67'	'00'	长度错误

下面分别再对作为基本应用外延的加油消费、本地解灰锁和联机解灰锁的交易
5 流程加以详细的说明。

1、加油交易：加油交易允许持卡人使用加油电子存折在卡—机联动的 IC 卡加油机上进行加油。此交易可以脱机进行。加油交易要求提交个人密码 (PIN)。参见附图 1 所示。

步骤 1.1：终端发出 INITIALIZE FOR PETROL 命令启动加油交易。

10 步骤 1.2：IC 卡收到 INITIALIZE FOR PETROL 命令后，处理 INITIALIZE FOR PETROL 命令，包括 (1) 检查 IC 卡是否处于灰锁状态，如果是，返回状态码 '6901' (不支持的密钥索引) 且不返回其他数据；(2) 检查命令中包含的密钥索引是否被 IC 卡支持，如果不支持，返回状态码 '9403' (不支持的密钥索引) 且不返回其他数据；(3) 通过以上检查之后，IC 卡将产生一个伪随机数 ICC、过程密钥 SESP
15 及报文鉴别代码 MAC1，过程密钥 SESP 被用于加油电子存折的加油交易，过程密钥按照 SESP=3EDS (DPK, DATA) 机制产生，其中 DPK 是加油电子存折的消费密钥，DATA 数据包括：伪随机数 ICC、加油电子存折脱机交易序号 CTC、终端交易序号 TTC 的最右两个字节，3DES 是指 3 倍长的 DES 运算。

SESPK 作用于以下数据进行 MAC1 的计算(按所列顺序):

——加油电子存折余额

——交易类型标识(加油交易为‘10’)

——终端机编号(发出 LOCK FOR PETROL 命令的终端)

5 步骤 1.3: 验证 MAC1

使用伪随机数 ICC 和 IC 卡返回的加油电子存折脱机交易序号, 加油消费安全认证模块 PSAM 将产生一样的过程密钥 SESPk 并验证 MAC1 是否有效, 如果 MAC1 有效, 交易处理将执行步骤 1.5, 如果 MAC1 无效, 交易处理继续执行步骤 1.4。

步骤 1.4: 回送错误状态, 终端应中止加油交易并采取相应的措施。

10 步骤 1.5: 产生 MAC2

终端确认能够进行加油交易后, 将产生一个报文认证码 MAC2, 供 IC 卡来验证 PSAM 的合法性。

SESPK 作用于以下数据进行 MAC2 的计算(按所列顺序):

——交易类型标识(加油交易为‘10’)

15 ——终端机编号(发出 LOCK FOR PETROL 命令的终端)

——交易日期(发出 LOCK FOR PETROL 命令的终端)

——交易时间(发出 LOCK FOR PETROL 命令的终端)

步骤 1.6: 终端发出 LOCK FOR PETROL 命令。

步骤 1.7: 验证 MAC2

20 收到 LOCK FOR PETROL 命令后, IC 卡要验证 MAC2 的有效性, 如果 MAC2 是有效的, 交易处理将继续执行步骤 1.8, 如果 MAC2 是无效的, 错误状态‘9302’(MAC 无效)被返回给终端。

步骤 1.8: 加油锁卡处理

25 IC 卡将伪随机数 ICC、终端机编号、终端交易序号、交易日期和交易时间写入内部文件, 以备加油中途 IC 卡掉电后的数据恢复, 并将加油电子存折置于灰锁状态, 禁止除加油消费和解灰锁以外的其他可能引起加油电子存折中余额变化的 IC 卡操作(如圈存、圈提、消费/取现、更改透支限额等)。当终端发送上述相关命令时, 错误状态‘6989’(卡已被灰锁)被返回给终端。

IC 卡将加油电子存折脱机交易序号加 1。

IC 卡产生一个报文鉴别码 MAC3 供 PSAM 对 IC 卡合法性进行检查, 并同时 will MAC3 写入内部文件。MAC3 将包含在从卡传送到 PSAM (通过终端) LOCK FOR PETROL 的命令响应报文和 GET GREY STATUS 的命令响应报文中。作为计算 MAC3 的输入, SESPCK 作用于以下数据进行 MAC3 计算:

- 5 ——加油电子存折余额
- 加油电子存折脱机交易序号 (加 1 前)
- 交易类型标识 (加油交易为 '10')
- 终端机编号 (发出 LOCK FOR PETROL 命令的终端)
- 交易日期 (发出 LOCK FOR PETROL 命令的终端)
- 10 ——交易时间 (发出 LOCK FOR PETROL 命令的终端)

IC 卡也应采用相同的机制直接用交易认证密钥 DTK 产生一个交易签名 TAC。并同时 will TAC 写入内部文件。TAC 将包含在从卡传送到 PSAM (通过终端) LOCK FOR PETROL 的命令响应报文和 GET GREY STATUS 的命令响应报文中。如果出现逃卡等意外情况使交易无法进行下去, TAC 将被写入终端交易明细, 以便后来传给主机进行

- 15 锁卡交易验证。下面是用来生成 TAC 的要素:

- 加油电子存折余额
- 加油电子存折脱机交易序号 (加 1 前)
- 交易类型标识
- 终端机编号
- 20 ——交易日期 (终端)
- 交易时间 (终端)

步骤 1.9: 验证 MAC3

终端要验证 MAC3 的有效性, 如果 MAC3 是有效的, 交易处理将继续执行步骤 1.10, 如果 MAC3 是无效的, 终端将采取相应措施。

- 25 步骤 1.10: 持卡人加油

在加油过程中, IC 卡允许被下电。若下电以后, IC 卡重新上电, 经过交易预处理 (验证密码, 选择应用) 后应可以继续执行步骤 1.11 而不受影响。

步骤 1.11: 产生 GMAC

加油消费安全认证模块 PSAM 用过程密钥 SESPCK 产生一个报文认证码 GMAC, 供

IC 卡来验证 PSAM 的合法性。

SESPK 作用于以下数据进行 GMAC 的计算（按所列顺序）：

——加油交易金额

步骤 1.12：终端发出 DEBIT FOR PETROL 命令。

5 步骤 1.13：验证 GMAC

收到 DEBIT FOR PETROL 命令后，IC 卡先验证终端提交的 IC 卡脱机交易序号 CTC 是否匹配，若失败直接出错返回，不影响出错计数器。

IC 卡要验证 GMAC 的有效性，如果 GMAC 是有效的，交易处理将继续执行步骤 1.14，如果 GMAC 是无效的，错误状态‘9302’（MAC 无效）被返回给终端，同时

10 IC 卡内部出错计数器减一，若出错计数器减到 0 则永久锁死 IC 卡以防止恶意试探。

步骤 1.14：交易处理

IC 卡从卡上的加油电子存折余额中减去加油消费的交易金额，并将加油电子存折从灰锁状态下恢复为正常状态。IC 卡必须全部成功地完成以上几个步骤或者一个也不完成，如果余额的更新或加油电子存折状态的恢复没有成功，交易明细也不应
15 被更新。

IC 卡产生一个报文验证码 MAC4 供 PSAM 对 IC 卡合法性进行检查。MAC4 包含在从 IC 卡传送到 PSAM（通过终端）的 DEBIT FOR PETROL 命令响应报文中。作为计算 MAC4 的输入，DPK 作用于这些数据进行 MAC4 计算：

——加油交易金额

20 ——交易类型标识

——终端机编号

——交易日期（主机）

——交易时间（主机）

IC 卡也应采用相同的机制直接用交易认证密钥 DTK 产生一个交易签名 TAC。TAC
25 将被写入终端交易明细，以便后来传给主机进行交易验证。下面是用来生成 TAC 的要素：

——交易金额

——交易类型标识

——终端机编号（发出 DEBIT FOR PETROL 命令的终端）

——终端交易序号（发出 DEBIT FOR PETROL 命令的终端）

——交易日期（发出 DEBIT FOR PETROL 命令的终端）

——交易时间（发出 DEBIT FOR PETROL 命令的终端）

IC 卡将用以下数据组成的一个记录更新交易明细。

5 ——加油电子存折脱机交易序号

——交易金额

——交易类型标识

——终端机编号（发出 DEBIT FOR PETROL 命令的终端）

——交易日期（发出 DEBIT FOR PETROL 命令的终端）

10 ——交易时间（发出 DEBIT FOR PETROL 命令的终端）

步骤 1.15：验证 MAC4

收到从 IC 卡（经过终端）传来的 MAC4 后，PSAM 要验证 MAC4 的有效性。MAC4 验证的结果被传送到终端以便采取必要的措施。

2、联机解灰锁交易

15 联机解灰锁交易允许持卡人将 IC 卡上被灰锁的加油电子存折补扣解锁（恢复到正常状态）。本交易必须在联机的银行终端上进行。持卡人必须提交 PIN 来完成解灰锁交易。

步骤 2.1：终端发出 INITIALIZE FOR UNLOCK 命令启动加油交易。

步骤 2.2：IC 卡收到 INITIALIZE FOR UNLOCK 命令后，处理 INITIALIZE FOR
20 UNLOCK 命令，包括（1）检查 IC 卡是否处于灰锁状态，如果不是，返回状态码‘6901’（无效的命令）且不返回其他数据。（2）检查命令中包含的密钥索引是否被 IC 卡支持，如果不支持，返回状态码‘9403’（不支持的密钥索引）且不返回其他数据。（3）通过以上检查之后，IC 卡将产生一个伪随机数 ICC、过程密钥 SESULKK 和一个报文认证码 MAC1，供主机来验证解灰锁交易和 IC 卡的合法性。过程密钥 SESULKK
25 被用于加油电子存折的解灰锁交易。过程密钥 SESULKK 是用解灰密钥 DULKK 与产生消费过程密钥相同的机制产生。用来产生过程密钥 SESULKK 的输入数据如下：

SESULKK：伪随机数 ICC||加油电子存折联机交易序号||‘8000’

SESULKK 作用于以下数据进行 MAC1 的计算（按所列顺序）：

——加油电子存折余额

——交易类型标识（解灰锁交易为‘11’）

——终端机编号

IC 卡将把 INITIALIZE FOR UNLOCK 命令的响应报文送给终端处理，如果 IC 卡返回的状态不是‘9000’，终端将终止交易。

- 5 在收到 INITIALIZE FOR UNLOCK 命令的响应报文后，终端将包含表 17 中数据的解灰锁许可请求报文送往发卡方主机。

步骤 2.3：验证 MAC1

主机将生成 SESULKK 并且确认 MAC1 是否有效，如果 MAC1 有效，交易处理将继续执行步骤 2.5，如果 MAC1 无效，交易处理将执行步骤 2.4。

- 10 步骤 2.4：回送错误状态

如果出现使解灰锁交易不能被接受的条件，则主机会通知终端。终端应采取相应的措施。

步骤 2.5：主机处理

- 15 在确认能够进行圈存交易后，主机会产生一个报文验证码 MAC2，供 IC 卡对主机合法性进行检查。SESULKK 作用于以下数据进行 MAC2 计算（按所列顺序）：

——补扣的交易金额

——交易类型标识

——终端编号

——交易日期（主机）

- 20 ——交易时间（主机）

主机发送一个解锁交易接受报文给终端，其中包括 MAC2、交易日期（主机）和交易时间（主机）。

步骤 2.6：终端收到主机的解锁交易接受报文后，终端会发出 DEBIT FOR UNLOCK 命令给 IC 卡以更新卡上加油电子存折余额并将加油电子存折恢复到正常状态。

- 25 步骤 2.7：验证 MAC2

收到 DEBIT FOR UNLOCK 命令后，IC 卡要验证 MAC2 的有效性，如果 MAC2 是有效的，交易处理将继续执行步骤 2.8，如果 MAC2 是无效的，错误状态‘9302’（MAC 无效）被返回给终端。

步骤 2.8：交易处理

IC 卡从卡上的加油电子存折余额中减去补扣的交易金额, 将加油电子存折联机交易序号加 1, 并将加油电子存折从灰锁状态下恢复为正常状态。IC 卡必须全部成功地完成以上几个步骤或者一个也不完成, 如果余额或序号的更新或加油电子存折状态的恢复没有成功, 交易明细也不应被更新。IC 卡产生一个报文验证码 MAC3 供主机对 IC 卡合法性进行检查。MAC3 包含在从卡传送到主机(通过终端)的 DEBIT FOR UNLOCK 命令响应报文中。SESULK 作用于以下数据进行 MAC3 计算:

- 加油电子存折余额
- 加油电子存折联机交易序号 (加 1 前)
- 补扣金额
- 交易类型标识
- 终端机编号
- 交易日期 (主机)
- 交易时间 (主机)

IC 卡也应采用相同的机制直接用交易认证密钥 DTK 产生一个交易签名 TAC。TAC 将被写入终端交易明细, 以便后来传给主机进行交易验证。下面是用来生成 TAC 的要素:

- 加油电子存折余额
- 加油电子存折联机交易序号 (加 1 前)
- 补扣金额
- 交易类型标识
- 终端机编号
- 交易日期 (主机)
- 交易时间 (主机)

IC 卡用以下数据组成的一个记录更新交易明细:

- 加油电子存折联机交易序号
- 补扣金额
- 交易类型标识
- 终端机编号
- 交易日期 (主机)

——交易时间（主机）

步骤 2.9：验证 MAC3

主机收到从 IC 卡（经过终端）传来的 MAC3 后，要验证 MAC3 的有效性，MAC3 验证成功则继续步骤 2.10，否则主机发给终端错误报文。

5 步骤 2.10：返回确认

在成功完成步骤 2.9 后，主机做相应的处理。

3、本地解灰锁交易

本地解灰锁交易允许持卡人将 IC 卡上被灰锁的加油电子存折补扣解锁（恢复到正常状态）。本交易必须在拥有上次逃卡记录的终端上进行。持卡人必须提交 PIN 来完成解灰锁交易。

步骤 3.1：终端发出 GET GREY STATUS 命令启动本地解灰锁交易。

步骤 3.2：IC 卡收到 GET GREY STATUS 命令后，处理 GET GREY STATUS 命令，IC 卡将电子存折的灰标志状态（GREY FLAG）、电子存折的余额、电子存折的联机交易序号、电子存折的脱机交易序号、锁卡时的 MAC3 和 TAC 通过 GET GREY STATUS 15 命令的响应报文返回给终端。

步骤 3.3：验证 MAC3

终端判断 IC 卡的电子存折是灰锁的情况下，将得到 MAC3 后与逃卡记录中的 MAC3 比较。

步骤 3.4：终端发出 DEBIT FOR PETROL 命令。

20 步骤 3.5：验证 GMAC

收到 DEBIT FOR PETROL 命令后，IC 卡先验证终端提交的 IC 卡脱机交易序号 CTC 是否匹配，若失败直接出错返回，不影响出错计数器。

IC 卡要验证 GMAC 的有效性，如果 GMAC 是有效的，交易处理将继续执行步骤 3.6，如果 GMAC 是无效的，错误状态‘9302’（MAC 无效）被返回给终端，同时 IC 25 卡内部出错计数器减一，若出错计数器减到 0 则永久锁死 IC 卡以防止恶意试探。

SESPK 作用于以下数据进行 GMAC 的计算：

——加油交易金额

步骤 3.6：交易处理

IC 卡从卡上的加油电子存折余额中减去加油消费的交易金额，并将加油电子存

折从灰锁状态下恢复为正常状态。IC 卡必须全部成功地完成以上几个步骤或者一个也不完成，如果余额的更新或加油电子存折状态的恢复没有成功，交易明细也不应被更新。

IC 卡产生一个报文验证码 MAC4 供 PSAM 对 IC 卡合法性进行检查。MAC4 包含在
5 从卡传送到 PSAM（通过终端）的 DEBIT FOR PETROL 命令响应报文中，作为计算 MAC4 的输入，DPK 作用于这些数据进行 MAC4 计算：

——加油交易金额

IC 卡也应采用相同的机制直接用交易认证密钥 DTK 产生一个交易签名 TAC。TAC 将被写入终端交易明细，以便后来传给主机进行交易验证。下面是用来生成 TAC 的

10 要素：

——交易金额

——交易类型标识

——终端机编号（发出 DEBIT FOR PETROL 命令的终端）

——终端交易序号（发出 DEBIT FOR PETROL 命令的终端）

15 ——交易日期（发出 DEBIT FOR PETROL 命令的终端）

——交易时间（发出 DEBIT FOR PETROL 命令的终端）

IC 卡将用以下数据组成的一个记录更新交易明细。

——加油电子存折脱机交易序号

——交易金额

20 ——交易类型标识

——终端机编号（发出 DEBIT FOR PETROL 命令的终端）

——交易日期（发出 DEBIT FOR PETROL 命令的终端）

——交易时间（发出 DEBIT FOR PETROL 命令的终端）

步骤 3.7：验证 MAC4

25 收到从 IC 卡（经过终端）传来的 MAC4 后，PSAM 要验证 MAC4 的有效性。MAC4 验证的结果被传送到终端以便采取必要的措施。

在本加油电子存折应用中，数据元定义包括：

1、交易类型标识：

- 10 ——加油消费
- 11 ——解灰锁
- 12 ——本地解灰锁

其他交易类型标识与现有技术同。

5 2、密钥关系

用于加油电子存折的特殊密钥，均为双倍长 DEA 密钥（128 比特长）。

密钥	发卡行	IC 卡	POS (PSAM)
用于解灰锁交易的 密钥	解 灰 锁 主 密 钥 (MULKK)	解灰锁子密钥（DULKK）， 由 MULKK 用应用序列号推导 获得。	N/A

其他的密钥关系请参照现有技术定义。

IC 卡内部指令状态变化包括：

1、加油电子存折的内部文件

- 10 每一个加油电子存折都有一个内部文件与其对应，该文件用于存放灰锁时的伪随机数 ICC、终端机编号、终端交易序号、交易日期、交易时间和 MAC2，该文件的内容应不受 IC 卡电源的影响，以供本地解锁时恢复锁卡时的密钥状态。

操作加油电子存折

2、IC 卡在收到对加油电子存折操作的命令后需要增加的内部操作：

- 15 ——检查该加油电子存折是否处于灰锁状态。如果不是，进入空闲状态。
- 如果是灰锁状态，IC 卡从内部文件中恢复上次锁卡时的伪随机数 ICC、终端机编号、终端交易序号、交易日期、交易时间和 MAC2，并通过恢复的数据和相同的机制恢复过程密钥 SESPk。

权利要求书

1、一种实现电子存折（钱包）安全交易的方法，其特征在于：将灰锁标记并入该电子存折（钱包），成为该电子存折（钱包）的属性参数之一；在灰锁 IC 卡即置灰锁标记的同时，将锁卡的来源记入 IC 卡；当扣款操作时执行对该锁卡来源的判断，并将扣款操作和解灰操作合并为 IC 卡上的一步操作，即扣款成功后自动解灰。

2、根据权利要求 1 所述的方法，其特征在于：更进一步的可在主机上保存有一条可以实现扣款、强制解灰操作的密钥，使灰锁后的 IC 卡可在联机的终端上通过联机方式实现补扣款及强制解灰操作。

3、根据权利要求 1 所述的方法，其特征在于建立的 IC 卡消费交易流程为：用户插卡、终端和 IC 卡双向认证、终端灰锁 IC 卡、消费、消费实现后终端从 IC 卡的电子存折（钱包）扣款并解灰锁。

4、根据权利要求 3 所述的方法，其特征在于所述的灰锁 IC 卡是指：IC 卡根据其锁卡的来源生成一认证码，同时将产生该锁卡来源的所需参数传递给终端，由终端采用与 IC 卡相同的机制产生另一锁卡来源码，并使用该锁卡来源码生成另一认证码，将该认证码送入 IC 卡，IC 卡判断与上述 IC 卡自身生成的认证码是否相同，若相同时执行灰锁操作并将这次产生的一灰锁特征码返回给终端，该灰锁特征码为根据其锁卡来源及相应信息在内的数据生成。

所述的终端从 IC 卡的电子存折（钱包）扣款并解灰锁是指：终端根据其锁卡来源和扣款所需的参数生成一认证码，将该认证码与相应参数一并送入 IC 卡，IC 卡内部采用其自身的锁卡来源和相同的参数通过相同的机制产生另一认证码，判断该认证码与终端产生的认证码一致就从 IC 卡的电子存折（钱包）上实现扣款，扣款成功的同时将灰标记清除。

5、根据权利要求 4 所述的方法，其特征在于：终端更进一步可将扣款时所需的认证码、这次的逃卡金额及灰锁特征码共同作为这次灰记录的部分信息保存起来，并上传给中心机；如果某次交易过程未完整结束的未被扣款解灰的 IC 卡，下一次在任何一个保存有该灰记录的终端上使用时，终端可先验证该灰锁特征码以确定 IC 卡上的锁卡来源与计算该条灰记录中的扣款认证码的锁卡来源相同，通过后执行

补扣款解灰操作。

6、 根据权利要求 1 所述的方法，其特征在于：所述的锁卡来源即为在 IC 卡上建立的一条过程密钥（SESPK），该过程密钥至少与一 IC 卡临时生成的伪随机数（ICC）相关。

5 7、 根据权利要求 5 所述的方法，其特征在于：所述的过程密钥（SESPK）=3DES（DPK，DATA），其中 DPK 是电子存折（钱包）的消费密钥，是由电子存折（钱包）消费主密钥（MPK）根据该 IC 卡的应用序号分散得到，DATA 是特定的参数，包括有所述的 IC 卡临时生成的伪随机数（ICC）、电子存折（钱包）的交易序号（CTC）、终端交易序号（TTC）的最后两个字节。

10 8、 根据权利要求 6 或 7 所述的方法，其特征在于：灰锁电子存折（钱包）时，终端将终端交易序号（TTC）送入 IC 卡，IC 卡获得自己的伪随机数（ICC）和电子存折（钱包）交易序号（CTC），内部建立过程密钥（SESPK），且将产生过程密钥（SESPK）的相应参数记录下来，产生这次灰锁特征码同时亦记录下来，将伪随机数（ICC）、电子存折（钱包）交易序号（CTC）发给终端，终端的安全认证模组
15 （PSAM）中存放有电子存折（钱包）消费主密钥（MPK），安全认证模组（PSAM）根据 IC 卡应用序号推导出 IC 卡上该电子存折（钱包）的 DPK，再根据伪随机数（ICC）、电子存折（钱包）交易序号（CTC）、终端交易序号（TTC），采用与 IC 卡相同的机制建立起相同的过程密钥（SESPK）；

扣款操作时终端使用该过程密钥（SESPK）根据扣款的金额、操作的日期时间
20 等计算出认证码，一并送入 IC 卡，IC 卡内部采用相同的数据和算法使用过程密钥（SESPK）同样计算出认证码，并与终端计算的结果相比较，相同则内部实现扣款和解灰，若认证码与终端计算的不同，内部不作扣款解灰操作，而将内部出错计数器增加，返回出错代码，如果内部出错计数器到达一定的次数，将 IC 卡的应用内部锁定以防止恶意的试探。

25 9、 根据权利要求 1 所述的方法，其特征在于：将灰锁标记并入电子存折（钱包）成为一特殊的加油电子存折（钱包）时，除具备通常的读余额、圈存、圈提、消费/取现、改透支限额等功能外，同时增加了加油消费、本地解灰锁和联机解灰锁功能。

10、 根据权利要求 9 所述的方法，其特征在于：描述该加油电子存折（钱包）

- 的状态除通常的空闲状态、圈存状态、消费/取现状态、圈提状态、修改状态外，还存在预加油状态、灰锁状态、和解灰锁状态，并在电子存折（钱包）通常的命令集中增加了加油初始化、加油锁卡、加油消费、解锁初始化、解锁、读取状态命令，其中，加油初始化命令用于初始化加油消费交易，加油锁卡命令用于灰锁加油消费
- 5 电子存折（钱包），加油消费命令用于本地加油消费交易同时解灰锁，解锁初始化命令用于初始化联机解灰锁消费交易，解锁命令用于联机解灰锁交易同时补扣加油消费，读取状态命令用于读取灰锁状态并启动本地解灰锁交易。

1/3

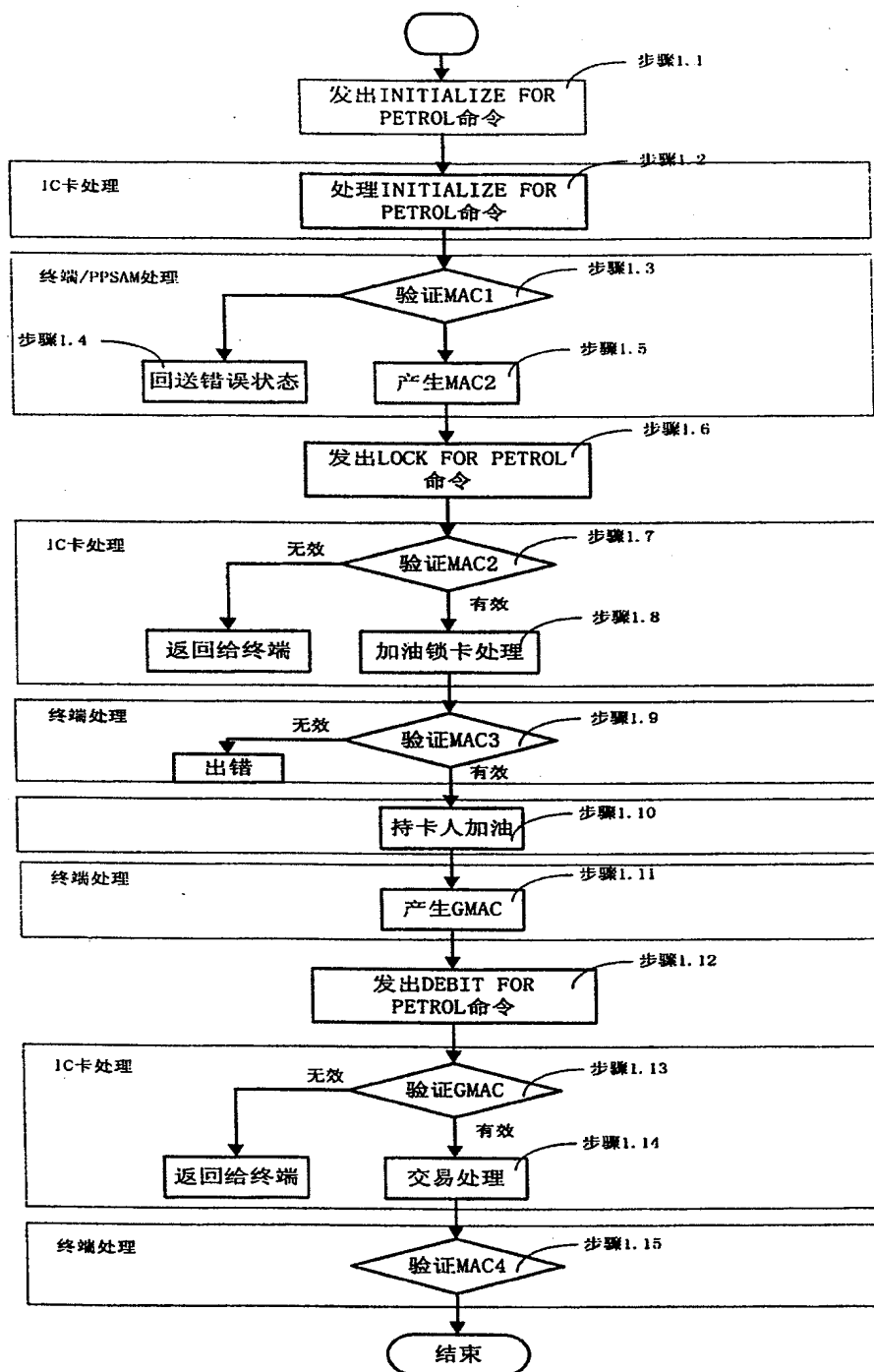


图 1

2/3

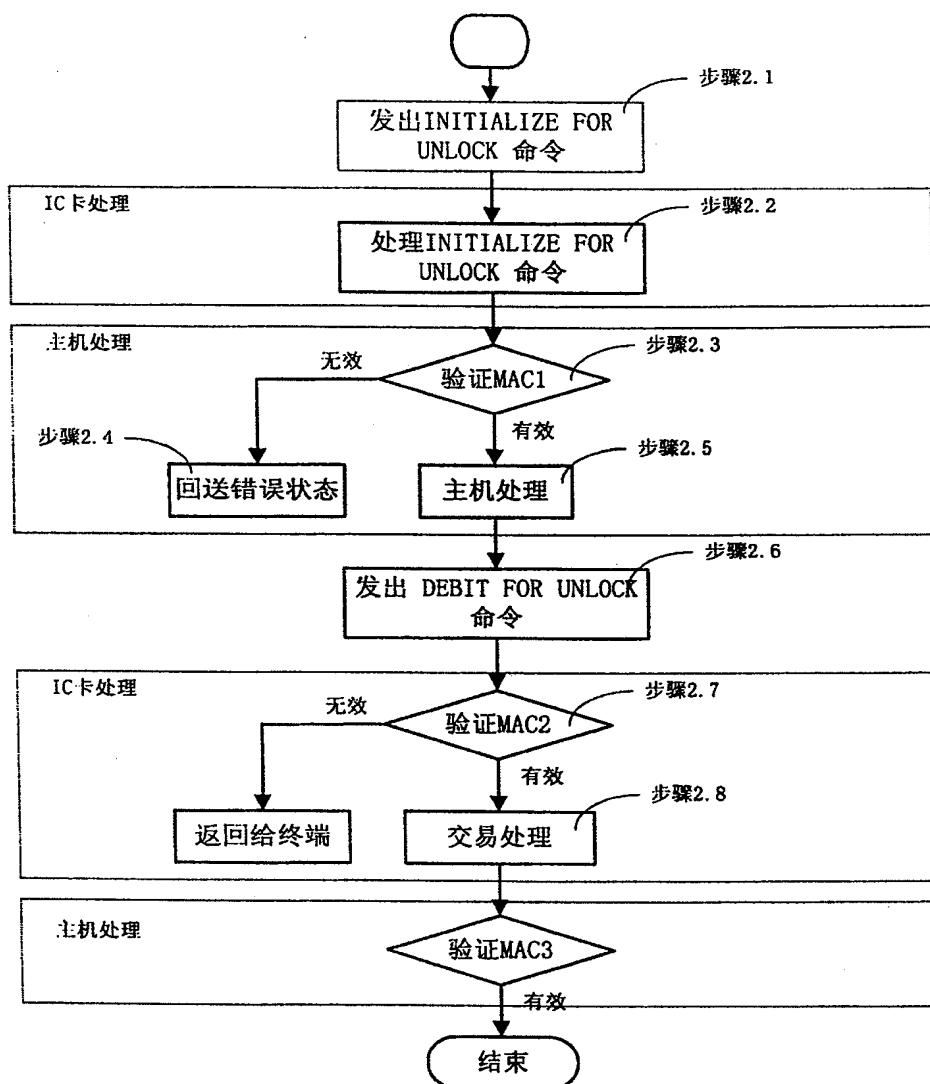


图 2

3/3

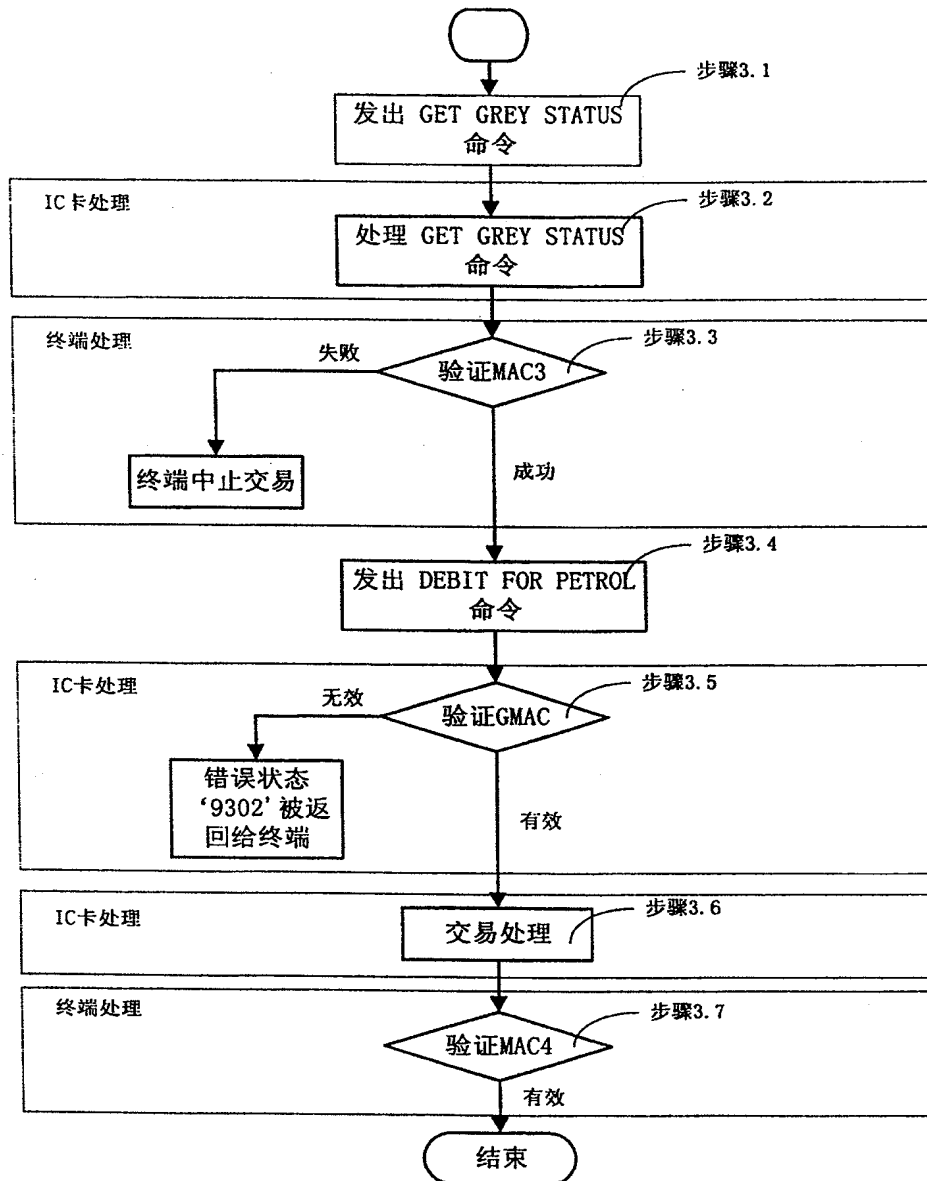


图 3